WE CLAIM

1. a method for authenticating validity of a public key certificate in compliance with a request, in a validation authority apparatus for certificates, said method comprising:

a step of searching for paths and validating the paths searched for, beforehand;

a path registration step of classifying the paths on the basis of a predetermined criterion in accordance with results of the searches and validations, and registering the classified paths in a database; and

a validity authentication step of receiving the request for authenticating the validity of the public key certificate, from a terminal device, and validating the public key certificate by using the paths registered beforehand.

2. A method for authenticating validity of a public key certificate as defined in claim 1, wherein:

in a case where, at the validity authentication step, any valid path corresponding to the validity authentication request is not registered, path search and validation are performed anew, thereby to authenticate the validity of the public key certificate.

3. A method for authenticating validity of a public key certificate as defined in claim 1, wherein:

the predetermined criterion at the path registration step classifies the paths into valid paths and invalid paths in accordance with the results of the validations; and

in a case where, at the validity authentication step, a path corresponding to the validity authentication request is registered as the valid path or the invalid path in the database, authentication of the validity of the public key certificate in the request is performed in accordance with the registered result.

4. A method for authenticating validity of a public key certificate as defined in claim 3, further comprising:

step of performing path validation in compliance with he validity authentication request so as to check if the pertinent public key certificate and the pertinent path observe any constraint item, in a case where, at the validity authentication step, the constraint item is described in the pertinent public key certificate or any public key certificate included in the pertinent path, although the path corresponding to the validity authentication request is registered as the valid path; and

step of judging the pertinent path as a valid path if the constraint item is observed.

5. A method for authenticating validity of a public key certificate as defined in claim 3, further comprising:

step of performing path validation in compliance with the validity authentication request so as to check if the pertinent public key certificate and the pertinent path observe any policy of an electronic procedure, in a case where, at the validity authentication step, the policy is described in the validity authentication request, the pertinent public key certificate or any public key certificate included in the pertinent path, although the path corresponding to the validity authentication request is registered as the valid path; and

step of judging the pertinent path as a valid path in a case where the policy is observed.

6. A method for authenticating validity of a public key certificate as defined in claim 3, wherein the path registration step comprises:

step of searching for each path which extends from a trust anchor certificate authority to a certificate authority that issues an end entity certificate;

step of acquiring and validating a certificate revocation list which concerns the end entity certificate, and which is issued by the certificate authority that issues the pertinent end entity certificate; and

step of registering the certificate revocation list together with a validation result thereof.

7. A method for authenticating validity of a public key certificate as defined in claim 6, wherein:

in a case where, at the validity authentication step, the path corresponding to the validity authentication request is registered as the valid path in the database, it is authenticated without validating the certificate revocation list that the pertinent public key certificate is not revoked.